Key Backup

Technology

KEY BACKUP TECHNOLOGY

- "Clone" technology originated as a "key backup" service, and has analogies in computer software copying

VC2000E	Software
- Crucial data stored as numbers in volatile RAM	- Crucial data stored as magnetic orientations on fragile disk media
- If battery dies, lightning strike, etc. crucial data can be lost	- Scratches on disk, head crashes, etc. loses crucial data

KEY BACKUP TECHNOLOGY

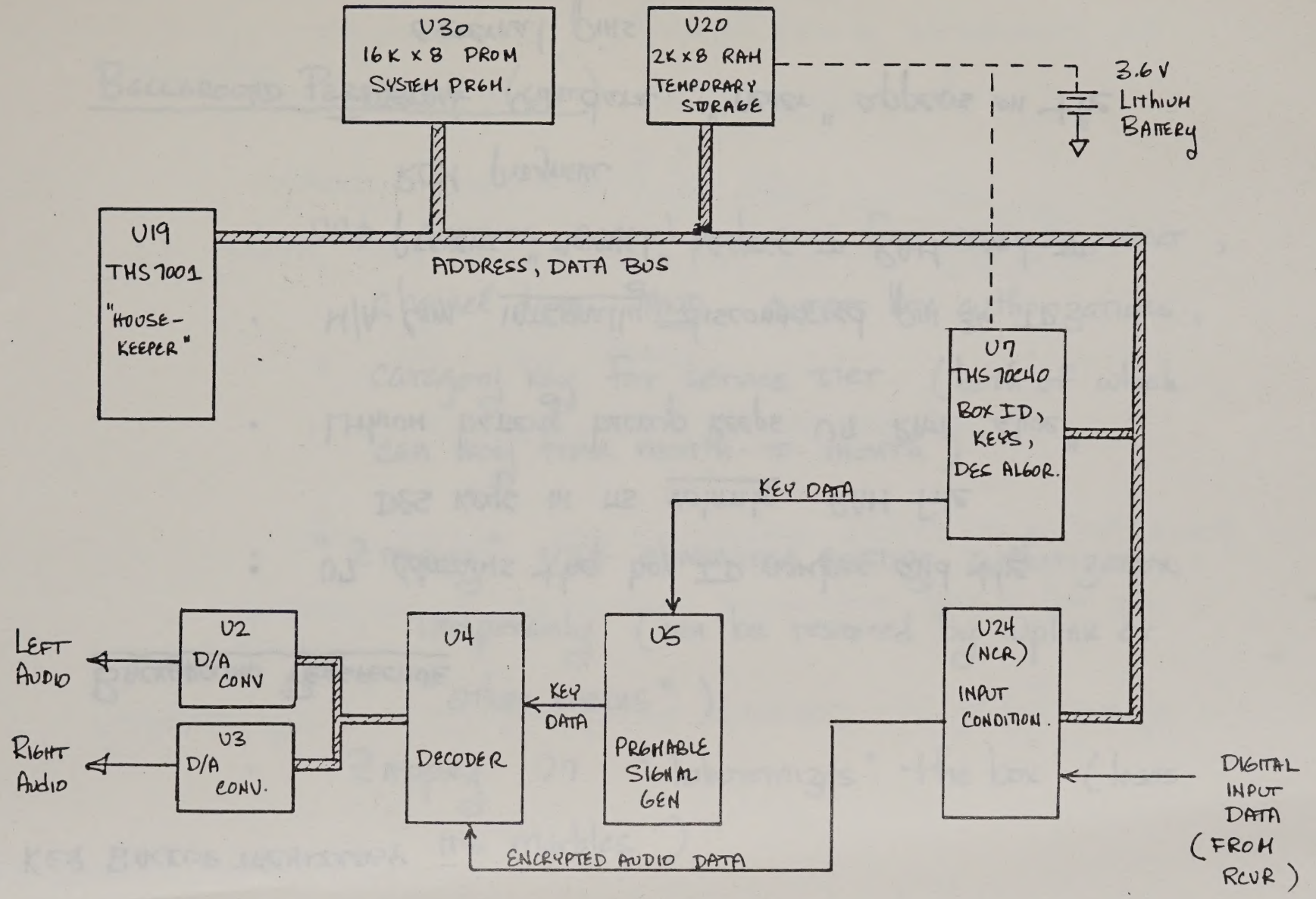
VC2000	Software
- vendors "copy protect" their data, depriving legitimate users of making backup	- vendors "copy protect" their data, depriving legitimate users of making backup
- techniques developed for extracting key data and keeping in archival storage	- "copy-busting" programs developed and marketed freely in open literature
- potential for abuse: cloning ID number into additional boxes of friends, etc. depriving vendor of potential revenue.	- potential for abuse: making copies of software for friends, etc. depriving vendor of potential revenue

- Legal aspects of cloning will be discussed in later talks

- This talk will include history of cloning in USA and demonstrations of hardware

- USE OF "CLONING CHIPS" for any purpose other than restoring life to your own VC2¢¢¢E IS OF QUESTIONABLE LEGALITY, SUBJECT TO ELABORATION BY LATER SPEAKERS

VC2000E
Simplified Block Diagram
Audio Computer Section



- KEY BACKUP TECHNOLOGY -

BACKGROUND PERSPECTIVE

- U7 contains the box ID number and the DES keys in its volatile RAM file.
- Lithium battery backup keeps U7 RAM "alive"
- M/A-Com internally disconnected pin 36 to prevent "normal" access to RAM. and to ROM program
- Internal U7 data "never" appears on the external pins

BACKGROUND PERSPECTIVE (CONT.)

- U2ϕ contains scratchpad area for messages, TEXT, channel data AND current box authorizations, category key for service tier (both of which can vary from month-to-month)
- "ZAPPING" U2ϕ eliminates existing authorization TEMPORARILY (can be restored by uplink or "other means")
- ZAPPING U7 "lobotomizes" the box (loses its marbles)

- KEY BACKUP TECHNOLOGY -

Milestone #1 : U7 ROM listing obtained (Spring 86)

- Unreadable by conventional techniques due to pin 36 open circuit, two alternative approaches were tried
  1. Laser microsurgery to reconnect pin 36
  2. Vcc / clock games
- Initial ROM readout may have been obtained by Texas group by reconnecting pin 36
- Approach #2 gave a partial ROM dump
- A "software hole" (probably part of an internal TI QC check) allowed ROM to easily be obtained after the fact (knowing the ROM pgm = seeing the hole)

KEY BACKUP TECHNOLOGY

MILESTONE #1 (CONT)

- UNFORTUNATELY, Vcc/clock games lost the U7 RAM contents, as did the "software" hole approach.

KEY BACKUP TECHNOLOGY

Milestone #2 : One set of DES keys extracted (Summer 86)

- By laser microsurgery on the U7 chip KEPT ALIVE BY THE BATTERY, PIN 36 was reconnected and one set of DES keys was extracted
- This allowed cloning of that ID number ad infinitum
- Not an economically viable method due to time and expenses of microsurgery

KEY BACKUP TECHNOLOGY

Milestone #3: DES keys extracted thru processing (Fall 86)

- By exercising portions of code from U30 and U7 and feeding the unit "hostile" data, an algorithmic approach to calculating the DES keys was discovered.

- Initially extensive computer power was required, but some simplifications were discovered to allow operation on an IBM enhanced PC.

- Technique is general enough so that plugging of supposed holes in software, potting, etc. will not stop this technique.

KEY BACKUP TECHNOLOGY

EMERGENCE OF "WRITER" chips

- FIRST appeared late October IN Mid-WEST
- Subsitoted for U30 (temporarily), used SETUP 2 TO WRITE new ID and Keys INTO U7
- UNIT would be put on-line and wait for a "hit", after which it would come on.

KEY BACKUP TECHNOLOGY

DEFINITION OF "HIT"

- PRIOR TO 10 NOVEMBER 1986, an authorization message to each box would be downlinked approximately every 2 hours
- This message contained the authorization word and the category key for both the current month and the next month
- "HIT" counter (# of hits) is displayed as the 2nd row, 1ST column of the SETUP 0 screen.

KEY BACKUP TECHNOLOGY

MILESTONE #4: FIRST Countermeasure by uplink (10 Nov 1986)

- Authorization messages ceased for about 36 hours
- New authorization "hits" contained only
  NEXT months authorization + category key,
  NOT the current monthly codes.
- "Clones" would get hit and <u>not</u> come on
  (Indicated authorization but no picture or sound)
- Immediate pirate counter-countermeasure:
  frustration, then "lightning" story.

KEY BACKUP TECHNOLOGY

MILESTONE #5: FIRST effective CCH by USERS (THANKSGIVING)

- Transfer of U2ϕ authorization data from U2ϕ master unit to "clone"
- Initial techniques used VIC-2ϕ or CoCo to extract data, store, then write to "clone" U2ϕ.
- No more waiting for "hits" - units came up instantly after U2ϕ was programmed.

KEY BACKUP TECHNOLOGY

MILESTONE #6 : Development of SUPERCLIP

- Initial writer clips had socket on top of a DIPCLIP
- SUPERCLIP has PCB with U30 subsitute, and 2K of extra RAM
- Appropriate software in subsitute U3ϕ transfered U2ϕ master to clip — clip then moved to clone, where U2ϕ code and keys were transfered to U2ϕ and U7

KEY BACKUP TECHNOLOGY

MILESTONE #7: DEVELOPMENT OF INSTANT WRITERS

- Both U7 keys and U2ϕ data from master box are prestored into substitute U3ϕ
- One key transfers all info to clone
- INSTANT WRITER R&M's have a maximum lifetime of 8 weeks, depending on when they were made.

KEY BACKUP TECHNOLOGY

Advantages

- No electronic counter-measure possible from uplink
- No hardware changes to VC2000E
- One authorization for large numbers of boxes

Disadvantages

- Possibility of human error
- Serial number exposed unless minor mods are done to box ("1" key)
- Probably illegal